Financial Cybercrime Task Force of Kentucky

Advisory

Nov. 16, 2015 ***Reference # A1115-01***

Subject: Check ATMs for Skimmers

The DFI's Financial Cybercrime Task Force of Kentucky (FCTFK) alerts the financial services industry in Kentucky about skimmers.

Background: Recently, there is has been an increase in skimmer incidents in Kentucky. Card skimming is when the card magnetic stripe details and PIN are captured at the ATM by a modified card reader known as a skimming device. The skimming device is placed on the ATM in such a way that disguises its presence but allows it to capture the information on the magnetic stripe of the card and the input of the customer's PIN. The customer inserts their card into the ATM that has been modified with a skimming device, performs a normal transaction, and retains the card. The customer leaves the ATM unaware that their card has been compromised. The captured information is then used to produce counterfeit cards for subsequent fraudulent cash withdrawals. The customer will only become aware of the fact when unauthorized cash withdrawals/transactions are made from their bank account. Because the skimming devices are very sophisticated, and often difficult to detect, multiple cards are compromised.

Recommendations: The Department urges state-chartered financial institutions to regularly inspect the card reader to make sure that it hasn't been tampered with and look for anything loose or damaged on the ATM. Financial institutions should take the following steps, as appropriate:

- Pull or gently tug on plastic card reader to make sure nothing comes loose. Also check for scratches around the card slot or adhesive tape or glue residue. The card reader should not scrape the card when it is inserted. Also check the keypad to make sure there is no false overlay.
- If anything seems out of place, contact the maintenance company for the ATM immediately.

- If tampering is evident or skimmers are suspected, notify local law enforcement immediately.
- ATMs that are more remote are more vulnerable. For customer safety ensure the area is free of obscuring structures and that the area is well-lit.
- Consider displaying warnings about skimming devices on or near the ATM along with details of a customer helpline to report incidents.
- Ensure security cameras are situated such that they record the area around the ATM, without actually being capable of recording any PIN number entered.
- Skimming activity often happens within a regional geographic area. If activity has been reported nearby, be extra vigilant.

Additional information on ATM skimming can be found at:

- FBI website at https://www.fbi.gov/news/stories/2011/july/atm_071411
- PCI Security Standards Council at https://www.pcisecuritystandards.org/documents/skimming_resource_guide.pdf

If you have any questions regarding this Alert, please contact dfi.reporting@ky.gov.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry. The Task Force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, http://kfi.ky.gov, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.